UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/599,052	07/06/2007	Mitch Webster	13421.1003	3554

20601 7590 05/18/2009
SPECKMAN LAW GROUP PLLC
1201 THIRD AVENUE, SUITE 330
SEATTLE, WA 98101

EXAMINER	
SALEHI, HELAI	

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
05/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/599,052	**Applicant(s)** WEBSTER ET AL.	
	Examiner HELAI SALEHI	**Art Unit** 2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09/18/06* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This is the initial office action has been issued in response to patent application, 10/599052, filed on 06 July 2007, with PCT date of 17 March 2005 and a foreign priority date of 17 March 2004. Claims 1-27, as originally amended and filed, are currently pending and have been considered below.

Minor Informalities

1. Claims 1, 10, 21, 24, and 25 are objected to because of the following informalities:

Claims 1, 10, and 21 recites “randomise said digitized genomic information” and “randomised information” which appears to be a misspelling of the word “randomize".

Claim 10 recites “providing a interim method”. Examiner suggest changing "a" to "an".

Claims 21 and 25 recites “genomic information whilst enabling” which appears to be a misspelling of the word "while".

Claim 21 recites "receiving authorisation" and “third party data request authorisation” which appears to be a misspelling of the word “authorization”.

Claim 24 recites “unauthorised third party data request” which appears to be a misspelling of the word “unauthorized”.

Claim 25 recites “an authorised third party" which appears to be a misspelling of the word "authorized".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-2, 4-16, 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ross et al. (US 7173148 B2, file date 10/20/04) in view of Robinson et al. (US 6581069 B1, patent date 06/17/03).

Claim 1:

With respect to claim 1, Ross et al. discloses a method for the secure storage of personal genomic information **(projection values representing an integral of activity within body of patient, Column 3, lines 11-15)** using a secure central database server residing within a sequencing service outlet **(using PET system, Figure 1)** comprising the steps of:

receiving and sequencing said individual's genomic sample to provide genomic information for said individual **(object being scanned by PET system and capturing plurality of detection elements, frame acquisition, Column 4, lines 17-22, Figure 2),** digitizing said genomic information **(data emitted and captured into frame, Column 4, lines 18-19, Figure 2)**, applying a splitting algorithm to fragment **(applying splitting algorithm to each frame, Column 6, lines 7-10, lines 54-57, Figure 6A-604)** and randomize said digitized genomic information and separating said fragmented and randomized information into at least two separate datasets **(splitting correction data corresponding to each frame that is split into plurality of subsets, Figure 6A-608, 604),**

storing the remainder of said datasets in a secure central database record **(projection frames may be stored in memory unit of system, Column 4, lines 6-7, Figure 1),** applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data and to provide said individual's genomic information in an informative format **(applying algorithm (6) to combine the ratio image data from each frame/subset and providing a final image, Column 7, lines 63-67, Column 8, (6) lines 30-31).**

Ross et al. does not disclose receiving and registering an individual's request to access and use said secure storage of personal genomic information system in a registration database and generating an interim unique identification code for said individual;
storing at least one of said datasets in at least one portable storage device to be retained by said individual;

activating said portable storage device by downloading an activation code from said secure central database server whereby said individual uses said interim unique identification code for authentication of their identity;

allocating to said individual a unique customer identifying code for customer identification and

authentication purposes where said unique customer identifying code is also allocated to said secure central database record relating to said individual and said unique customer identification code is also allocated to said individual's personal record residing in said registration database;

receiving a request from said individual to reconstruct said individual's genomic information wherein said request includes said individual's customer identification code and log- on details;

authenticating said individual's request using said customer identification code and said log-on details and comparing the input data with said registration database;

downloading said individual's personal dataset from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server;

uploading a secure central database record, identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during user authentication, from said secure central database under the control of said sequencing service outlet;

combining the data from said portable storage device with the data from said secure central database record as claimed.

However Robinson et al. teaches receiving and registering an individual's request to access and use said secure storage of personal genomic information system in a registration database **(customer enters service contract, customer profiling information are entered into service contract database, Column 6, lines 16-21)** and generating an interim unique identification code for said individual **(customer must upload a user ID and password/access code into security server to access all reports, Column 7, lines 20-24),**

storing at least one of said datasets in at least one portable storage device to be retained by said individual **(scanner may be a portable device since the scanner is used interchangeable with medical imaging device and may be remotely located. The scanner may also be implemented in PET systems thus the storing of at least one of said datasets of Ross et al. may be in portable device (scanner) Column 1, lines 27-28, 40-48, Column 2, lines 21-23),**

activating said portable storage device by downloading an activation code from said secure central database server whereby said individual uses said interim unique identification code for authentication of their identity **(activating data logging functionality in a scanner by uploading user ID and password/access code into security server wherein the user ID and password/access code authenticates user identity, Column 3, lines 19-21, Column 7, lines 17-32),** allocating to said individual a unique customer identifying code for customer identification and

authentication purposes where said unique customer identifying code is also allocated to said secure central database record relating to said individual and said unique customer identification code is also allocated to said individual's personal record residing in said registration database **(allocating to customer a user ID and password/access code which must be uploaded to security server. Security server validates user via user ID and password/access code. Also customer profiling information is entered into service contract database, Column 7, lines 17-32, Column 6, lines 16-21),**

receiving a request from said individual to reconstruct said individual's genomic information wherein said request includes said individual's customer identification code and log- on details (**customer enters into service contract (request) to receive scanner utilization reports based on logged data (reconstruction), the customer must upload user ID and password/access code (Column 6, lines 16-21, Column 7, lines 20-24),**

authenticating said individual's request using said customer identification code and said log-on details and comparing the input data with said registration database **(validating users and comparing customer profiling information from service contract database, Column 7, line 25, Column 6, lines 16-27),** downloading said individual's personal dataset from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

(data logging file (personal dataset) arrives from scanner (portable storage device) to operation server, Column 6, lines 45-48),

uploading a secure central database record, identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during user authentication, from said secure central database under the control of said sequencing service outlet **(assigning access privileges based on reports (records within report server), identified by user ID and password/access code based on validation via security server under control of operation server, Column 7, lines 17-32, Figure 2-14, 22),**

combining the data from said portable storage device with the data from said secure central database record **(scanner may be a portable device since the scanner is used interchangeable with medical imaging device and may be remotely located. The scanner may also be implemented in PET systems thus the storing of at least one of said datasets of Ross et al. may be in portable device (scanner) Column 1, lines 27-28, 40-48, Column 2, lines 21-23). Ross et al. teaches datasets may be in stored secure database record (i.e. see Ross et al. projection frames may be stored in memory unit of system, Column 4, lines 6-7, Figure 1), thus the data may be within portable storage device and within central database.**

It would have been obvious to one skilled in the art at the time of the invention was made to use Robinson et al. in Ross for the steps of receiving and registering access request, storing and activating dataset in portable storage device, allocating and authenticating a unique customer identifying code, downloading dataset and uploading database record as claimed for purposes of maximizing data transactions and protection thus producing reliable and understandable images (data) within demanding schedules and over a considerable useful life (see Robinson, Column 1, lines 49-52).

Ross et al. and Robinson et al. are analogous art because they are from the same field of endeavor of positron emission tomography (PET) systems.

Claim 2:

With respect to claim 2, the combination of Ross et al. and Robinson et al. discloses the limitations of claim 1, as discussed above.

Robinson et al. discloses said secure central database record resides on a server which is accessed and controlled by a sequencing service outlet **(security server, Figure 2)** whereby said secure central database record is accessible on receipt of a data request from said individual using said unique customer identification code **(customer enters service contract, customer profiling information are entered into service contract database, Column 6, lines 16-21)** to authenticate their identity **(validating users and comparing customer profiling information from service contract database,**

Column 7, line 25, Column 6, lines 16-27) and downloading said individual portable storage device dataset into said server **(data logging file (personal dataset) arrives from scanner (portable storage device) to operation server, Column 6, lines 45-48).**

__Claims 4 and 18:__

With respect to claims 4 and 18, the combination of Ross et al. and Robinson et al. discloses the limitations of claims 1 and 10, as discussed above.

Robinson et al. discloses said sequencing service outlet server records account transactions for each registered individual **(every time customer enters into service contract, service features are provided to service contract database by central service facility, Column 6, lines 16-21).**

__Claims 5 and 19:__

With respect to claims 5 and 19, the combination of Ross et al. and Robinson et al. discloses the limitations of claims 4 and 18, as discussed above.

Robinson et al. discloses said account transactions are downloaded into hard copy format and forwarded to said individual **(extraction output file, Column 8, lines 47-57, Column 18-23, Tables 1-3, Figure 3-38).**

Claims 6 and 20:

With respect to claims 6 and 20, the combination of Ross et al. and Robinson et al. discloses the limitations of claims 1 and 10, as discussed above.

Robinson et al, discloses at least two portable storage devices are forwarded to said individual whereby one portable storage device is activated and the second portable storage device is retained by said individual in a de-activated form for back-up purposes **(the platform for multiple remote scanners permits clinicians and radiologist to operate a variety of scanners in different modalities and report issues of scanners thus examiner holds that at least two portable storage devices (scanner) reports can be forwarded to customers whereby one may be activated and other is retained in de-activated form for back up purpose Column 2, lines 19-29).**

Claim 7:

With respect to claim 7, the combination of Ross et al. and Robinson et al. discloses the limitations of claim 1, as discussed above.

Robinson et al. discloses said unique identification code is in label form for tracking said individual's genomic sample and providing an interim method by which said individual can authenticate their identity **(customer must upload a user ID and**

password/access code into security server to access all reports and security server validates user, Column 7, lines 20-25)

<u>Claims 8 and 14:</u>

With respect to claims 8 and 14, the combination of Ross et al. and Robinson et al. discloses the limitations of claim 1, as discussed above.

Robinson et al. discloses said genomic sample is taken from/received said individual by a DNA sequencing provider or a pathology service provider **(offering physician a range of techniques for imaging types of tissue, organs, physiological systems, Column 1, lines 27-32).**

<u>Claim 9:</u>

With respect to claim 9, the combination of Ross et al. and Robinson et al. discloses the limitations of claim 8, as discussed above.

Robinson et al. discloses said pathology service provider requests said unique sample identification code label from said sequencing service outlet server for attachment to said individual's genomic sample **(physicians draw upon PET resources as required by particular patient needs and when new exam, scanner output comprises CPT code, Column 1, lines 32-35, Column 5, lines 48-55, Column 6, lines 53-54).**

<u>**Claim 10:**</u>

With respect to claim 10, Ross et al. discloses a method for the secure storage of personal genomic information **(projection values representing an integral of activity within body of patient, Column 3, lines 11-15)** with a sequencing service outlet having a secure central server **(using PET system, Figure 1)** comprising the steps of: formatting said individual's genomic information such that said genomic information is amenable to the application of a splitting algorithm **(data emitted and captured into frame, allowing projection data to be acquired from multiple axial angles, Column 4, lines 17-25, Figure 2)**,

applying a splitting algorithm to fragment **(applying splitting algorithm to each frame, Column 6, lines 7-10, lines 54-57, Figure 6A-604)** and randomize said digitized genomic information

and separating said fragmented and randomized information into at least two separate datasets **(splitting correction data corresponding to each frame that is split into plurality of subsets, Figure 6A-608, 604),** such that, in the absence of any one dataset, the remainder of the datasets present uninformative information **(the subsets are needed to be combined and reconstructed to iteratively generate final image, Column 6, lines 10-12),**

storing the remainder of said datasets in a secure central database record **(projection frames may be stored in memory unit of system, Column 4, lines 6-7, Figure 1),** applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data and to provide said individual's genomic information in an informative format **(applying algorithm (6) to combine the ratio image data from each frame/subset and providing a final image, Column 7, lines 63-67, Column 8, (6) lines 30-31).**

Ross et al. does not disclose registering in a registration database an individual's request for use of said secure storage of personal genomic information;
generating two copies of a unique sample identification code in label form for tracking said individual's genomic sample and providing an interim method by which said individual can authenticate their identity,
receiving said individual's genomic information having one of said unique identification labels attached
storing at least one of said datasets in at least one portable storage device to be retained by said individual;
providing said portable storage device to said individual;
receiving a log-on request from said individual;
authenticating said individual using the log-on details and said interim method of authenticating said individual's identity by comparing the input data with said registration database, and approving log-on when authentication is successful;
receiving a request for portable storage device activation when said individual uses said sample identification code for re-authentication of their identity;

activating said portable storage device by downloading an activation code to said portable storage device;

allocating to said individual a unique customer identifying code for customer identification; and

authentication purposes where said unique customer identifying code is also allocated to said secure central database record relating to said individual and said unique customer identification code is also allocated to said individual's personal record residing in said registration database;

receiving a request from said individual to reconstruct said individual's genomic information wherein said request includes said individual's customer identification code and log- on details;

authenticating said individual's request using said customer identification code and said log-on details; and comparing the input data with said registration database;

downloading said individual's personal dataset from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server;

uploading a secure central database record, identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during user authentication, from said secure central database under the control of said sequencing service outlet

combining the data from said portable storage device with the data from said secure central database record as claimed.

However Robinson et al. teaches registering in a registration database an individual's request for use of said secure storage of personal genomic information **(customer enters service contract, customer profiling information are entered into service contract database, Column 6, lines 16-21)**,

generating two copies of a unique sample identification code in label form for tracking said individual's genomic sample and providing a interim method by which said individual can authenticate their identity,

(customer must upload a user ID and password/access code (2 copies) into security server to access all reports and security server validates user, Column 7, lines 20-25)

receiving said individual's genomic information having one of said unique identification labels attached **(scanner output comprises a system ID which is a unique ID for a particular customer, Column 5, lines 42-44),**

storing at least one of said datasets in at least one portable storage device to be retained by said individual **(scanner may be a portable device since the scanner is used interchangeable with medical imaging device and may be remotely located. The scanner may also be implemented in PET systems thus the storing of at least one of said datasets of Ross et al. may be in portable device (scanner) Column 1, lines 27-28, 40-48, Column 2, lines 21-23),**

providing said portable storage device to said individual **(scanner coupled to customer, Figure 1),** receiving a log-on request from said individual **(customer enters into service contract (request) to receive scanner utilization reports based on logged data (reconstruction), the customer must upload user ID and password/access code (Column 6, lines 16-21, Column 7, lines 20-24),**

authenticating said individual using the log-on details and said interim method of authenticating said individual's identity by comparing the input data with said registration database, and approving log-on when authentication is successful **(validating users and comparing customer profiling information from service contract database, Column 7, line 25, Column 6, lines 16-27)**,

receiving a request for portable storage device activation when said individual uses said sample identification code for re-authentication of their identity **(customers can access the reports periodically provided they have inputted a valid and authentic security factors, ID and password (Column 5, lines 21-30),**

activating said portable storage device by downloading an activation code to said portable storage device **(activating data logging functionality in a scanner by uploading user ID and password/access code into security server, Column 3, lines 19-21)**,

allocating to said individual a unique customer identifying code for customer identification' and

authentication purposes where said unique customer identifying code is also allocated to said secure central database record relating to said individual and said unique customer identification code is also allocated to said individual's personal record residing in said registration database **(allocating to customer a user ID and password/access code which must be uploaded to security server. Security server validates user via user ID and password/access code. Also customer profiling information is entered into service contract database, Column 7, lines 17-32, Column 6, lines 16-21),**

receiving a request from said individual to reconstruct said individual's genomic information wherein said request includes said individual's customer identification code and log- on details (**customer enters into service contract (request) to receive scanner utilization reports based on logged data (reconstruction), the customer must upload user ID and password/access code (Column 6, lines 16-21, Column 7, lines 20-24),**

authenticating said individual's request using said customer identification code and said log-on details and comparing the input data with said registration database **(validating users and comparing customer profiling information from service contract database, Column 7, line 25, Column 6, lines 16-27),**

downloading said individual's personal dataset from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server **(data logging file (personal dataset) arrives from scanner (portable storage device) to operation server, Column 6, lines 45-48),**

uploading a secure central database record, identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during user authentication, from said secure central database under the control of said sequencing service outlet **(assigning access privileges based on reports (records within report server), identified by user ID and password/access code based on validation via security server under control of operation server, Column 7, lines 17-32, Figure 2-14, 22),** and

combining the data from said portable storage device with the data from said secure central database record **(scanner may be a portable device since the scanner is used interchangeable with medical imaging device and may be remotely located. The scanner may also be implemented in PET systems thus the storing of at least one of said datasets of Ross et al. may be in portable device (scanner) Column 1, lines 27-28, 40-48, Column 2, lines 21-23). Ross et al. teaches datasets may be in stored secure database record (i.e. see Ross et al. projection frames may be stored in memory unit of system, Column 4, lines 6-7, Figure 1), thus the data may be within portable storage device and within central database.**

It would have been obvious to one skilled in the art at the time of the invention was made to use Robinson et al. in Ross for the steps of receiving and registering access request, storing and activating dataset in portable storage device, allocating and authenticating a unique customer identifying code, downloading dataset and uploading database record as claimed for purposes of maximizing data transactions and protection thus producing reliable and understandable images (data) within demanding schedules and over a considerable useful life (see Robinson, Column 1, lines 49-52).

Ross et al. and Robinson et al. are analogous art because they are from the same field of endeavor of positron emission tomography (PET) systems.

Claim 11:

With respect to claim 11, the combination of Ross et al. and Robinson et al. discloses the limitations of claim 10, as discussed above.

Robinson et al. discloses said registration database resides within the sequencing service outlet server **(service contract database coupled to scanner, Figure 2, 30, 2).**

Claim 12:

With respect to claim 12, the combination of Ross et al. and Robinson et al. discloses the limitations of claim 10, as discussed above.

Robinson et al. discloses said genomic information, having said unique sample identification code attached, is received from said individual **(scanner output of exam data includes patient ID, Column 5, lines 48-50).**

Claim 13:

With respect to claim 13, the combination of Ross et al. and Robinson et al. discloses the limitations of claim 10, as discussed above.

Robinson et al. discloses said genomic information, having said unique sample identification code attached is received from a third party **(exam data which includes patient ID also includes information provided by third party, i.e. referring ID, operator ID, exam description, series, and type (Column 5, lines 48-54).**

Claims 15 and 16:

With respect to claims 15 and 16, Ross et al. discloses said formatting of said individual's genomic information comprises sequencing and the digitization of said genomic information **(data emitted and captured into frame, allowing projection data to be acquired from multiple axial angles, Column 4, lines 17-25, Figure 2)**.

3. Claims 3 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ross et al. (US 7173148 B2, file date 10/20/04) in view of Robinson et al. (US 6581069 B1, patent date 06/17/03) and further in view of Su (US 2003/0232346 A1, publish date 12/18/03).

Claims 3 and 17:

With respect to claims 3 and 17, the combination of Ross et al. and Robinson et al. discloses the limitations of claims 1 and 10, as discussed above.

Ross et al. discloses said at least two datasets include an individual’s genomic information **(PET system creates frames/subsets of integral activity within the body, Column 3, lines 11-15)** and reconstruction algorithm residing within said sequencing service outlet secure central database server **(applying algorithm (6) to combine the ratio image data from each frame/subset and providing a final image, Column 7, lines 63-67, Column 8, (6) lines 30-31).**

Robinson et al. discloses a reconstruction key required to initiate said reconstruction algorithm **(a unique key for the scanner, Column 5, lines 44-45).**

Neither Ross et al. nor Robinson et al. discloses an individual's genomic information comprising nucleotide sequence information and/or annotation information generated from or relating to said individual's genetic sample as claimed.

However, Su teaches techniques capable of detecting and identifying nucleotide may be used, i.e. positron emission tomography. **(Page 3, 0029, lines 9-13)**

It would have been obvious to one skilled in the art at the time of the invention was made to use Su in Ross et al. and Robinson et al. for at least the two databases include an individual’s genomic information comprising nucleotide sequence information and/or annotation information generated from or relating to said individual's genetic sample as claimed for purposes of allowing the database sets to comprise of genetic sampling and thus maximizing the protection of data transactions.

Ross et al., Robinson et al., and Su are analogous art because they are from the same field of endeavor of positron emission tomography (PET) systems.

4. Claims 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ross et al. (US 7173148 B2, file date 10/20/04) in view of Robinson et al. (US 6581069 B1, patent date 06/17/03) and further in view of Yasuda et al. (US 2005/0069874 A1, file date 11/30/00).

Claim 21:

With respect to claim 21, Ross et al. discloses a method for the secure storage of personal genomic information **(projection values representing an integral of activity within body of patient, Column 3, lines 11-15)** whilst enabling non-anonymous transactions with a sequencing service outlet **(using PET system, Figure 1)** for third party access to all or fragments of an individual's genomic information comprising the steps of:

applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data from said portable device with the data from said secure central database record to reproduce said individual's genomic information in an informative format **(applying algorithm (6) to combine the ratio image data from each frame/subset and providing a final image, Column 7, lines 63-67, Column 8, (6) lines 30-31).**

applying a splitting algorithm to fragment and randomize said digitized genomic information and separating said fragmented **(applying splitting algorithm to each frame, Column 6, lines 7-10, lines 54-57, Figure 6A-604)** and randomized information into at least two separate datasets **(splitting correction data corresponding to each frame that is split into plurality of subsets, Figure 6A-608, 604** such that, in the absence of any one dataset, the remainder of the datasets presents uninformative information **(the subsets are needed to be combined and reconstructed to iteratively generate final image, Column 6, lines 10-12),**

storing the remainder of said datasets in a secure public dataset database record under the control of said sequencing service outlet **(projection frames may be stored in memory unit of system, Column 4, lines 6-7, Figure 1),**

applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data and to provide said individual's genomic information in an informative format **(applying algorithm (6) to combine the ratio image data from each frame/subset and providing a final image, Column 7, lines 63-67, Column 8, (6) lines 30-31).**

Ross et al. does not disclose receiving a third party request for access to personal genomic information or fragments thereof, generating a unique third party customer identification code thereby providing a method by which said third party can authenticate their identity,

receiving a log-on request from said individual,

authenticating said individual using the log-on details and a customer identification code input by said individual,

comparing the input data with the registration database data, and approving log-on when authentication is successful,

receiving a third party transaction request from said individual, recording said third party transaction request in a third party request database, generating a unique third party transaction code for said request, providing said third party transaction code to said individual,

authenticating said third party identity by comparing said third party customer identification code and said third party contact information provided in said third party data request with details residing in said third party registration database, and approving third part access on successful completion of authentication, receiving authorization for said third party request from said individual,

uploading a secure central database record identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during third party data request authorization, from said secure central database under the control of said sequencing service outlet, downloading said individual's personal dataset information from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

generating a data identification code as an access label for said datasets,

storing at least one of said datasets in a third party portable storage device,

providing said third party portable storage device to said third party, activating said third party portable storage device where said third party uses said data identification code and said third party customer identification code for authentication of their identity and an activation code is downloaded to said third party portable storage device,

receiving a request from said third party to reconstruct said individual's genomic information or portions thereof where said request includes said third party customer identification code and log-on details,

authenticating said third party request using said third party identification code, third party transaction code and said log-on details and comparing the input data with said third party registration database,

downloading said individual's personal dataset from said third party portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

uploading a secure public dataset record, identified by said third party transaction code and being identical to said third party transaction identification code entered by said third party during third party authentication, from said secure public database under the control of said sequencing service outlet,

combining the data from said portable storage device with the data from said secure central database record as claimed.

However Robinson et al. teaches receiving a third party request for access to personal genomic information or fragments thereof **(customer enters service contract to receive reports based on logged data Column 6, lines 16-21),**

generating a unique third party customer identification code thereby providing a method by which said third party can authenticate their identity **(customer must upload a user ID and password/access code into security server to access all reports, Column 7, lines 20-24),**

receiving a log-on request from said individual (**customer enters into service contract (request) to receive scanner utilization reports based on logged data (reconstruction), the customer must upload user ID and password/access code (Column 6, lines 16-21, Column 7, lines 20-24),**

authenticating said individual using the log-on details and a customer identification code input by said individual **(validating users and comparing customer profiling information from service contract database, Column 7, line 25, Column 6, lines 16-27),** and

comparing the input data with the registration database data, and approving log-on when authentication is successful **(validating users and comparing customer profiling information from service contract database and assigning access privileges, Column 7, line 25-27, Column 6, lines 16-27)**, and receiving a third party transaction request from said individual, recording said third party transaction request in a third party request database, generating a unique third party transaction code for said request, providing said third party transaction code to said individual **(customer enters into service contract (request) to receive scanner utilization reports based on logged data (reconstruction), the customer must upload user ID and password/access code (Column 6, lines 16-21, Column 7, lines 20-24), (validating users and comparing customer profiling information from service contract database, Column 7, line 25, Column 6, lines 16-27)**,

authenticating said third party identity by comparing said third party customer identification code and said third party contact information provided in said third party data request with details residing in said third party registration database, and approving third part access on successful completion of authentication

(assigning access privileges based on reports (records within report server), identified by user ID and password/access code based on validation via security server under control of operation server, Column 7, lines 17-32, Figure 2-14, 22),

receiving authorization for said third party request from said individual **(security server validating users and comparing customer profiling information from service contract database, Column 7, line 22-25, Column 6, lines 16-27)**,

uploading a secure central database record identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during third party data request authorization, from said secure central database under the control of said sequencing service outlet **(assigning access**

privileges based on reports (records within report server), identified by user ID and password/access code based on validation via security server under control of operation server, Column 7, lines 17-32, Figure 2-14, 22),

downloading said individual's personal dataset information from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server **(data logging file (personal dataset) arrives from scanner (portable storage device) to operation server, Column 6, lines 45-48),**

generating a data identification code as an access label for said datasets **(customer must upload a user ID and password/access code (2 copies) into security server to access all reports and security server validates user, Column 7, lines 20-25)**

storing at least one of said datasets in a third party portable storage device **(scanner may be a portable device since the scanner is used interchangeable with medical imaging device and may be remotely located. The scanner may also be implemented in PET systems thus the storing of at least one of said datasets of Ross et al. may be in portable device (scanner) Column 1, lines 27-28, 40-48, Column 2, lines 21-23),** and

providing said third party portable storage device to said third party, activating said third party portable storage device where said third party uses said data identification code and said third party customer identification code for authentication of their identity and an activation code is downloaded to said third party portable storage device **(activating data logging functionality in a scanner by uploading user ID and password/access code into security server wherein the user ID and**

password/access code authenticates user identity, Column 3, lines 19-21, Column 7, lines 17-32),

receiving a request from said third party to reconstruct said individual's genomic information or portions thereof where said request includes said third party customer identification code and log-on details **(customer enters into service contract (request) to receive scanner utilization reports based on logged data (reconstruction), the customer must upload user ID and password/access code (Column 6, lines 16-21, Column 7, lines 20-24),**

authenticating said third party request using said third party identification code, third party transaction code and said log-on details and comparing the input data with said third party registration database **(validating users and comparing customer profiling information from service contract database, Column 7, line 25, Column 6, lines 16-27)** ,

downloading said individual's personal dataset from said third party portable storage device using a machine-readable computer interface device, to said sequencing service outlet server **(data logging file (personal dataset) arrives from scanner (portable storage device) to operation server, Column 6, lines 45-48),**

uploading a secure public dataset record, identified by said third party transaction code and being identical to said third party transaction identification code entered by said third party during third party authentication, from said secure public database under the control of said sequencing service outlet,

(assigning access privileges based on reports (records within report server), identified by user ID and password/access code based on validation via security server under control of operation server, Column 7, lines 17-32, Figure 2-14, 22), combining the data from said portable storage device with the data from said secure central database record **(scanner may be a portable device since the scanner is used interchangeable with medical imaging device and may be remotely located. The scanner may also be implemented in PET systems thus the storing of at least one of said datasets of Ross et al. may be in portable device (scanner) Column 1, lines 27-28, 40-48, Column 2, lines 21-23). Ross et al. teaches datasets may be in stored secure database record (i.e. see Ross et al. projection frames may be stored in memory unit of system, Column 4, lines 6-7, Figure 1), thus the data may be within portable storage device and within central database.**

Neither Ross et al. nor Robinson et al. discloses logging said request in a third party registration database residing within the sequencing service outlet server,
receiving a third party data request from said third party which includes third party contact information, details at least the genes or genomic sequence interval and/or genomic information or portions thereof of said individual's genomic information required, to said sequencing service outlet server using said third party transaction code and said third party customer identification code for authentication of said third party, posting of said third party data request to a data repository residing within said sequencing service outlet server for access and approval by said individual,

isolating said genes or genomic sequence interval and/or genomic information or portions thereof of said genomic information according to said third party data request as claimed.

However, Yasuda et al. teaches logging said request in a third party registration database residing within the sequencing service outlet server **(analysis request order sheet within Figure 9),**

receiving a third party data request from said third party which includes third party contact information, details at least the genes or genomic sequence interval and/or genomic information or portions thereof of said individual's genomic information required, to said sequencing service outlet server using said third party transaction code and said third party customer identification code for authentication of said third party **(receiving a service request from customer to gene access center, authorized third party Page 4, 0040, lines 1-6),**

posting of said third party data request to a data repository residing within said sequencing service outlet server for access and approval by said individual **(receiving request from customer who requests analytic order for analysis of genomic information from access server under control of gene information access center (Page 2, 0025, lines 1-3, Figure 9)**

isolating said genes or genomic sequence interval and/or genomic information or portions thereof of said genomic information according to said third party data request

(analytic results, Figure 10),

It would have been obvious to one skilled in the art at the time of the invention was made to use Yasuda et al. in Ross et al. and Robinson et al. for the steps of logging request from said third party detailing of the genes or genomic sequence interval and/or genomic information or portions thereof of said individual's genomic information required, to said sequencing service outlet server using said third party transaction code and said third party customer identification code for authentication of said third part posting of said third party data request, isolating said genes or genomic sequence interval and/or genomic information or portions thereof as claimed for purposes of enhancing the versatility of the system for options of both authorized data records or anonymous records options and therefore maximizing the security of the system.

Ross et al., Robinson et al., and Yasuda et al. are analogous art because they are from the same field of endeavor of personal genomic information and authentication.

Claim 22:

With respect to claim 22, the combination of Ross et al., Robinson et al., and Yasuda et al. discloses the limitations of claim 21, as discussed above.

Yasuda et al. discloses said third party non-anonymous transactions are available to medical laboratory, medical research, and medical diagnostic purposes and/or health care and/or medical insurance providers who register with said sequence service outlet **(medical treatment organization, analysis and information, Figure 1).**

Claim 23:

With respect to claim 23, the combination of Ross et al., Robinson et al., and Yasuda et al. discloses the limitations of claim 21, as discussed above.

Yasuda et al. discloses said data request includes said third party transaction code, said third party identification code, information relating to at least details of the genes or genomic sequence interval and/or genomic information requested by said third party and business contact details of said third party **(analysis request, Figure 9).**

Claim 24:

With respect to claim 24, the combination of Ross et al., Robinson et al., and Yasuda et al. discloses the limitations of claim 21, as discussed above.

Yasuda et al. disclose said data request termination notice is posted to said third party on receipt of an unauthorized third party data request **(customer registration section transmits individual identification code/password in order to access customer screen via internet thus examiner holds that a termination notice (i.e. access denied) is posted to said third party when unauthorized identification code/password is received Page 2, 0026, lines 57, Page 3, 0026, lines 1-3).**

Claim 25:

With respect to claim 25, Ross et al. discloses a method for the secure storage of personal genomic information **(projection values representing an integral of activity within body of patient, Column 3, lines 11-15)** whilst enabling anonymous transactions with a sequencing service outlet **(using PET system, Figure 1)** for third party access to whole genome sequences or fragments of an individual's genomic information comprising the steps of:

applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data and to provide said individual's genomic information in an informative format **(applying algorithm (6) to combine the ratio image data from each frame/subset and providing a final image, Column 7, lines 63-67, Column 8, (6) lines 30-31).**

Ross et al. does not disclose receiving, authenticating and approving if successful, a log-on request from said individual using said individual's computer log-on details and a customer identification comparing the data input with a registration database residing on a server in said sequencing service outlet,

downloading personal dataset information from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

uploading of a secure central database record identified by said individual's customer identification code, from a secure central database under the control of said sequencing service outlet,

receiving, authenticating and approving if successful, a log-on request from a third party to provide using a third party identification code input by said third party and comparing the input data with a third party registration database record under the control of said sequencing service outlet,

uploading a third party public access database record corresponding to said third party data request and providing said third party public access to database record to said third party,

combining the data from said portable storage device with the data from said secure central database record as claimed.

However, Robinson et al. discloses receiving, authenticating and approving if successful, a log-on request from said individual using said individual's computer log-on details and a customer identification comparing the data input with a registration database residing on a server in said sequencing service outlet **(validating users based on customer upload of user ID and password or access code and comparing customer profiling information from service contract database, Column 7, lines 20-25, Column 6, lines 16-27)**,

downloading personal dataset information from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server **(data logging file (personal dataset) arrives from scanner (portable storage device) to operation server, Column 6, lines 45-48),**

uploading of a secure central database record identified by said individual's customer identification code, from a secure central database under the control of said sequencing service outlet **(assigning access privileges based on reports (records within report server), identified by user ID and password/access code based on validation via security server under control of operation server, Column 7, lines 17-32, Figure 2-14, 22),**

receiving, authenticating and approving if successful, a log-on request from a third party to provide using a third party identification code input by said third party and comparing the input data with a third party registration database record under the control of said sequencing service outlet **(customer enters into service contract (request) to receive scanner utilization reports based on logged data (reconstruction), the customer must upload user ID and password/access code (Column 6, lines 16-21, Column 7, lines 20-24), (validating users and comparing customer profiling information from service contract database, Column 7, line 25, Column 6, lines 16-27)**,

uploading a third party public access database record corresponding to said third party data request and providing said third party public access to database record to said third party **(assigning access privileges based on reports (records within report server) which are available to customer, identified by user ID and**

password/access code based on validation via security server under control of operation server, Column 7, lines 17-32, Figure 2-14, 22).

combining the data from said portable storage device with the data from said secure central database record **(scanner may be a portable device since the scanner is used interchangeable with medical imaging device and may be remotely located. The scanner may also be implemented in PET systems thus the storing of at least one of said datasets of Ross et al. may be in portable device (scanner) Column 1, lines 27-28, 40-48, Column 2, lines 21-23). Ross et al. teaches datasets may be in stored secure database record (i.e. see Ross et al. projection frames may be stored in memory unit of system, Column 4, lines 6-7, Figure 1), thus the data may be within portable storage device and within central database.**

Neither Ross et al. nor Robinson et al. discloses receiving an information disclosure form request from said individual detailing at least details of the genes or genomic sequence interval and/or genomic information or portions thereof to be made available for access by an authorized third party,

isolating and downloading said genes or genomic sequence interval and/or genomic information or portions thereof from said genomic information according to said information disclosure form request to a third party public access database record residing on a third party public access server under the control of said sequencing service outlet in a format such that said third party public access database record is anonymous having no link to a real world identity, receiving a third party data request detailing at least the details of the genes or genomic sequence interval and/or genomic information or portions thereof required, to said sequencing service outlet server as claimed.

However, Yasuda et al. teaches request from said individual detailing at least details of the genes or genomic sequence interval and/or genomic information or portions thereof to be made available for access by an authorized third party **(receiving a service request from customer to gene access center, authorized third party Page 4, 0040, lines 1-6),**

isolating and downloading said genes or genomic sequence interval and/or genomic information or portions thereof from said genomic information according to said information disclosure form request to a third party public access database record residing on a third party public access server under the control of said sequencing service outlet in a format such that said third party public access database record is anonymous having no link to a real world identity **(analytic order screen (form request) allows for analysis of genomic information from third party public access server under control of gene information access center such that database record can have no links to actual customer information (i.e. choosing to select gene information service, Function of gene. Figure 9, Figure 4, Page 5, 0061, 0061),**

receiving a third party data request detailing at least the details of the genes or genomic sequence interval and/or genomic information or portions thereof required, to said sequencing service outlet server **(receiving request from customer who requests analytic order for analysis of genomic information from access server under control of gene information access center (Page 2, 0025, lines 1-3, Figure 9).**

It would have been obvious to one skilled in the art at the time of the invention was made to use Yasuda et al. in Ross et al. and Robinson et al. for the steps of request from said individual detailing of the genes or genomic sequence interval and/or genomic information or portions thereof to be made available for access by an authorized third party, isolating and downloading said genes such that said third party public access database record is anonymous having no link to a real world identity, receiving a third party data request detailing at least the details of the genes or genomic sequence interval and/or genomic information or portions thereof required, to said sequencing service outlet server as claimed for purposes of enhancing the versatility of the system for options of both authorized data records or anonymous records options and therefore maximizing the security of the system.

Ross et al., Robinson et al., and Yasuda et al. are analogous art because they are from the same field of endeavor of personal genomic information and authentication.

Claim 26:

With respect to claim 26, the combination of Ross et al., Robinson et al., and Yasuda et al. discloses the limitations of claim 25, as discussed above.

Yasuda et al. discloses said anonymous third party transactions are used for medical laboratory, medical research and/or medical diagnostic purposes **(medical treatment organization, analysis and information, Figure 1).**

<u>Claim 27:</u>

With respect to claim 27, the combination of Ross et al., Robinson et al., and Yasuda et al. discloses the limitations of claim 25, as discussed above.

Yasuda et al. discloses said information disclosure form request includes a survey to enable third parties to collect relevant phenotype information **(analytical results: gene name and arrangement, Figure 10).**

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure, Wheeler JR et al. (US 2006/0210131 A1).

Wheeler JR et al. is cited for the teaching of projection image data and reconstruction algorithm, Figure 4)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HELAI SALEHI whose telephone number is (571) 270-7468. The examiner can normally be reached on Monday - Friday from 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/HELAI SALEHI/

Examiner, Art Unit 2433

/Carl Colin/

Primary Examiner, Art Unit 2433